# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-138671
(43)Date of publication of application : 16.05.2000

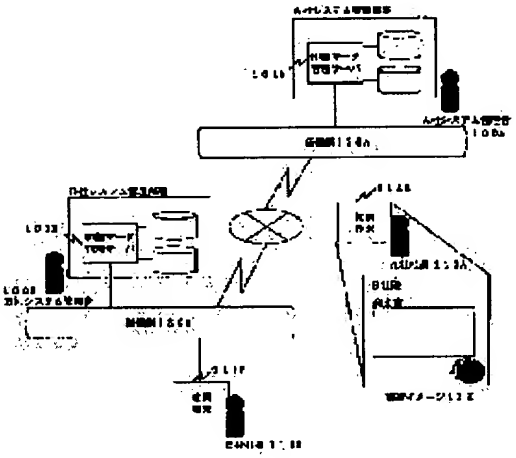
(51)Int.Cl. H04L 9/32
G06F 17/60
G06T 7/00
G09C 1/00
G09C 5/00

(21)Application number : 10-309806
(22)Date of filing : 30.10.1998

(71)Applicant : HITACHI LTD
(72)Inventor : TSUCHIYAMA CHIKAKO
TOYOSHIMA HISASHI
NAGAI YASUHIKO

## (54) ELECTRIC SEAL MARK AUTHENTICATION

(57)Abstract:
PROBLEM TO BE SOLVED: To identify a correct person and data at the time of transmitting and receiving digital data by adding a mark in which personal identification information and digital data authentication information are included in a mark design to digital data so as to authenticate digital data through the use of authentication information in the mark.
SOLUTION: A clerk terminal 111A displays digital data with a seal mark stuck to it. When a clerk 110A clicks the authentication button of the seal mark, the authentication item section of the seal mark is displayed. When the clerk 110A clicks the personal authentication item of the seal mark, a seal mark authentication processing part extracts personal authentication information from the seal mark. It is collated whether an open key for decoding extracted personal authentication information matches with an open key stored in the terminal 111, etc. When it matches, a seal mark authentication processing part displays personal authentication information in a processing picture image so as to confirm contents by decoding personal information extracted from the seal mark and authenticates.



LEGAL STATUS
[Date of request for examination] 26.08.2003
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－138671
（P2000－138671A）
(43)公開日　平成12年５月16日(2000.5.16)

| (51)Int.Cl.' | | 識別記号 | FI | | | テーマコード'（参考） |
|---|---|---|---|---|---|---|
| Ｈ０４Ｌ | 9/32 | | Ｈ０４Ｌ | 9/00 | ６７３Ｄ | ５Ｂ０４３ |
| Ｇ０６Ｆ | 17/60 | | Ｃ０９Ｃ | 1/00 | ６６０Ｂ | ５Ｂ０４９ |
| Ｇ０６Ｔ | 7/00 | | | 5/00 | | ５Ｊ１０４ |
| Ｇ０９Ｃ | 1/00 | ６６０ | Ｃ０６Ｆ | 15/21 | Ｚ | |
| | 5/00 | | | 15/62 | ４５５ | |

審査請求　未請求　請求項の数10　ＯＬ　（全 18 頁）　最終頁に続く

(21)出願番号　特願平10－309806

(22)出願日　平成10年10月30日(1998.10.30)

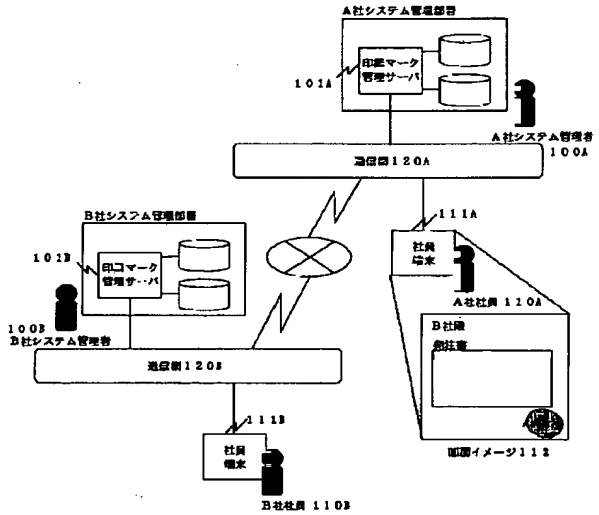
(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　土山　千佳子
神奈川県川崎市幸区鹿島田890番地　株式会社日立製作所システム開発本部内
(72)発明者　豊島　久
東京都江東区新砂一丁目６番27号　株式会社日立製作所公共情報事業部内
(74)代理人　100083552
弁理士　秋田　収喜

最終頁に続く

(54)【発明の名称】　電子印鑑マーク認証システム

(57)【要約】
【課題】　ネットワーク上でデジタルデータを送受信する際の本人認証及びデータ認証を実現することが可能な技術を提供する。
【解決手段】　印影または署名を表すマークによりデジタルデータの認証を行うマーク管理サーバにおいて、マークの新規登録または更新を要求するマーク登録要求をマーク端末装置から受信し、要求元の人物を認証する為の情報を暗号鍵で暗号化した本人認証情報を当該要求元のマークデザインに埋め込んでマークを作成し、前記作成したマークに前記本人認証情報を復号化する為の復号鍵を添付して要求元に配布するマーク管理処理部と、前記暗号化した本人認証情報を復号化する為の復号鍵をマーク復号鍵管理ＤＢに登録し、前記登録した復号鍵を各マーク端末装置に送信するマーク復号鍵管理処理部とを備えるものである。

図１



【特許請求の範囲】
【請求項１】　印影または署名を表すマークによりデジタルデータの認証を行うマーク管理サーバにおいて、
マークの新規登録または更新を要求するマーク登録要求をマーク端末装置から受信し、要求元の人物を認証する為の情報を暗号鍵で暗号化した本人認証情報を当該要求元のマークデザインに埋め込んでマークを作成し、前記作成したマークに前記本人認証情報を復号化する為の復号鍵を添付して要求元に配布するマーク管理処理部と、
前記暗号化した本人認証情報を復号化する為の復号鍵をマーク復号鍵管理ＤＢに登録し、前記登録した復号鍵を各マーク端末装置に送信するマーク復号鍵管理処理部とを備えることを特徴とするマーク管理サーバ。
【請求項２】　前記マーク管理処理部は、本人認証情報が埋め込まれていることを示す視認性を可視透かしにより前記マークに持たせることを特徴とする請求項１に記載されたマーク管理サーバ。
【請求項３】　前記マーク管理処理部は、マーク付加時に送信されるログ情報をマークログ管理ＤＢに格納するものであることを特徴とする請求項１または請求項２のいずれかに記載されたマーク管理サーバ。
【請求項４】　印影または署名を表すマークによりデジタルデータの認証を行うマーク端末装置において、
マークの新規登録または更新を要求するマーク登録要求をマーク管理サーバに送信し、要求元の人物を認証する為の情報を暗号鍵で暗号化した本人認証情報を当該要求元のマークデザインに埋め込んで作成したマークをマーク管理サーバから受け取るマーク登録処理部と、
本人認証情報を復号化する為の復号鍵をマーク管理サーバから受信し、前記復号鍵を復号鍵ＤＢに格納する復号鍵格納処理部とを備えることを特徴とするマーク端末装置。
【請求項５】　印影または署名を表すマークによりデジタルデータの認証を行うマーク端末装置において、
マークが付加されるデジタルデータの特徴情報を含むデジタルデータ認証情報とマーク付加通算番号とをユーザ固有の暗号鍵で暗号化し、本人認証情報が埋め込まれたマークに前記暗号化されたデジタルデータ認証情報及びマーク付加通算番号を埋め込み、前記デジタルデータの選択された位置に前記マークを付加するマーク付加処理部を備えることを特徴とするマーク端末装置。
【請求項６】　前記マーク付加処理部は、デジタルデータ認証情報が埋め込まれていることを示す視認性を可視透かしにより前記マークに持たせることを特徴とする請求項５に記載されたマーク端末装置。
【請求項７】　前記マーク付加処理部は、マーク付加時にログ情報をマーク管理サーバに送信するものであることを特徴とする請求項５または請求項６のいずれかに記載されたマーク端末装置。
【請求項８】　印影または署名を表すマークによりデジタルデータの認証を行うマーク端末装置において、
デジタルデータに付加されたマークから本人認証情報を抽出し、その本人認証情報を復号化する為に添付された復号鍵が復号鍵ＤＢに格納されている復号鍵と合致するかどうか照合し、前記復号鍵が合致している場合には前記マークから抽出した本人認証情報を前記復号鍵で復号化して本人認証情報を表示し、合致していない場合にはエラーメッセージを表示するマーク認証処理部を備えることを特徴とするマーク端末装置。
【請求項９】　印影または署名を表すマークによりデジタルデータの認証を行うマーク端末装置において、
デジタルデータに付加されたマークからデジタルデータ認証情報を抽出して復号鍵により復号化し、マークが付加されているデジタルデータから特徴情報を抽出し、前記デジタルデータから抽出した特徴情報とマークから抽出したデジタルデータ認証情報中の特徴情報とを比較照合し、特徴情報が合致している場合には前記デジタルデータ認証情報の表示を行い、合致していない場合にはエラーメッセージを表示するマーク認証処理部を備えることを特徴とするマーク端末装置。
【請求項１０】　前記マーク認証処理部は、認証処理でエラーが発生した場合に当該マークを無効なデザインに変更するものであることを特徴とする請求項８または請求項９のいずれかに記載されたマーク端末装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明はデジタルデータを電子的なマークにより認証する電子マーク認証システムに関し、特にデジタルデータを印影や署名を表す電子マークにより認証する電子マーク認証システムに適用して有効な技術に関するものである。
【０００２】
【従来の技術】ネットワーク上での商取引等が広がりつつある現在、伝達する情報の確からしさをネットワーク上で確認できる技術が重要になってきている。第３者が成りすましていないかを確認する本人認証については、「ＣａｒｄＷａｖｅ　‘９８年３月号」でＥＣＯＭ（電子商取引実証推進協議会）の本人認証技術検討Ｇが各種の方式を分類しており、パスポートやクレジットカード等による所有物を利用する方式、指紋、声紋や筆跡等のバイオメトリクスを利用する方式、パスワードやデジタル署名等の秘密情報を利用する方式等があるが、ネットワークで用いる場合には所有物や秘密情報を用いる方式が一般的である。
【０００３】また、情報の途中改ざんの確認については、インターネットを利用したＥＣ(Electronic Commerce)で、クレジット決済を安全に行う為に用いられるＳＥＴ(Secure Electronic Transactions)では、デジタル署名によるカード所有者の認証を行っている。デジタル署名は、通常伝達したい情報を圧縮した圧縮文を送り手

の暗号鍵で暗号化した暗号文であり、送り手の復号鍵（公開鍵）で元の圧縮文に復号化できる。つまり、受け手は受け取ったメッセージから作った圧縮文と受け取ったデジタル署名から復号化した圧縮文とを比較することで、メッセージが改ざんされていないかの確認、つまり文書認証ができる。

【０００４】一方、印鑑や署名が一般的に持つ意味合いは、本人認証と文書認証を合わせ持つと考えられる。従来の印鑑を電子化した電子印鑑システムはいくつか製品化されている。これらの製品により、社内での決済文書等において、印影イメージを用いて承認を行うことができる。中にはＩＤ管理による押印時のセキュリティ管理や、サーバでの押印履歴管理による不正コピー防止の機能を提供する製品もある。また特開平１０－１１５０９号公報の様に、印鑑やサイン等を文書に付加し、その形等を文書の特徴量で変形させ、その認証を可能にすることにより、文書の改ざんを防止することも考えられている。

【０００５】

【発明が解決しようとする課題】デジタル署名は文書認証と本人認証の両方の機能を有するとも言えるが、文書等のデジタルデータの受け手はそのデジタルデータを見ただけでは、情報の正当性や送り手の確認をすることはできない。現実社会では実印の押印の様に見て確認できるものによって安心感を感じることがあるが、デジタル署名はこの様な視認性を持たないと言える。

【０００６】一方、従来の電子印鑑システムでは目で見て確認できる印影を用いるが、印影自体は単なるデザインであって、文書等デジタルデータの受け手が送り手を確認するにはログ情報等の履歴を調べる必要があった。

【０００７】また特開平１０－１１５０９号公報に記載された技術においても印影自体は単なるデザインデータであって、文書認証を行う為にはサーバ上の基準となる印影と文書の特徴量で変形させた印影とを比較する必要がある。つまり、例えば特定のイントラネット内におけるオンラインでの本人認証や文書認証はできるが、企業間のネットワーク、例えばエクストラネット等でのデジタルデータのやり取りにおいて、デジタルデータの受け手が、表示されたデジタルデータ上でその内容や送り手の確認をすることができる機能を備えている電子印鑑システムはなかったと言える。

【０００８】また、従来のシステムの印影デザインは定型デザインの中から選ぶものである。つまり、例えば実社会で使用している印鑑やサインのデザインを印鑑システム上で使用することはできなかった。更に、視認性のある従来の電子印鑑システムとデジタル署名の両者を併用することは可能だが、それぞれを管理、運用する為には利用者・運用者共に煩雑な手順が必要となる。

【０００９】本発明の目的は上記問題を解決し、ネットワーク上でデジタルデータを送受信する際の本人認証及びデータ認証を実現することが可能な技術を提供することにある。

【００１０】

【課題を解決するための手段】印影または署名を表すマークによりデジタルデータの認証を行う電子マーク認証システムにおいて、マークデザインに本人認証情報及びデジタルデータ認証情報を埋め込んだマークをデジタルデータに付加し、マーク中の認証情報を用いて当該デジタルデータの認証を行うものである。

【００１１】本発明のマーク端末装置のマーク登録処理部が電子印鑑等のマークの新規登録または更新を要求するマーク登録要求をマーク管理サーバに送信すると、マーク管理サーバのマーク管理処理部は、マーク登録要求を受信し、要求元の人物を認証する為の情報を暗号鍵で暗号化した本人認証情報を当該要求元の印影デザイン等のマークデザインに埋め込んでマークを作成し、前記作成したマークに前記本人認証情報を復号化する為の復号鍵を添付して要求元に配布する。

【００１２】またマーク管理サーバのマーク復号鍵管理処理部は、前記暗号化した本人認証情報を復号化する為の復号鍵をマーク復号鍵管理ＤＢに登録し、前記登録した復号鍵を各マーク端末装置に送信する。

【００１３】マーク端末装置のマーク登録処理部は、マーク管理サーバのマーク管理処理部から送信されたマークを受け取り、また各マーク端末装置の復号鍵格納処理部は、マーク復号鍵管理処理部から送信された復号鍵を受信して復号鍵ＤＢに格納する。

【００１４】マーク端末装置のマーク付加処理部は、マークが付加される文書等のデジタルデータについて、その特徴情報を含むデジタルデータ認証情報とマーク付加通算番号とをユーザ固有の暗号鍵で暗号化し、当該デジタルデータを送信するユーザの本人認証情報が埋め込まれたマークに前記暗号化されたデジタルデータ認証情報及びマーク付加通算番号を埋め込み、前記デジタルデータの選択された位置に前記マークを付加する。

【００１５】前記の様にマークが付加されたデジタルデータが他のユーザのマーク端末装置に送信されると、そのマーク端末装置のマーク認証処理部は、デジタルデータに付加されたマークから本人認証情報を抽出し、その本人認証情報を復号化する為に添付された復号鍵が復号鍵ＤＢに格納されている復号鍵と合致するかどうか照合し、前記復号鍵が合致している場合には前記マークから抽出した本人認証情報を前記復号鍵で復号化して本人認証情報を表示し、合致していない場合にはエラーメッセージを表示する。

【００１６】またマーク端末装置のマーク認証処理部は、デジタルデータに付加されたマークからデジタルデータ認証情報を抽出して復号鍵により復号化し、マークが付加されているデジタルデータから特徴情報を抽出し、前記デジタルデータから抽出した特徴情報とマーク

から抽出したデジタルデータ認証情報中の特徴情報とを比較照合し、特徴情報が合致している場合には前記デジタルデータ認証情報の表示を行い、合致していない場合にはエラーメッセージを表示する。

【００１７】以上の様に本発明の電子マーク認証システムによれば、本人認証情報及びデジタルデータ認証情報を埋め込んで作成したマークをデジタルデータに付加し、マーク中の認証情報を用いて当該デジタルデータの認証を行うので、ネットワーク上でデジタルデータを送受信する際の本人認証及びデータ認証を実現することが可能である。

【００１８】

【発明の実施の形態】以下に企業イントラネット及び企業間ネットワークにおいて電子印鑑を用いて本人認証及び文書認証を行う一実施形態の電子マーク認証システムについて説明する。

【００１９】図１は本実施形態の電子印鑑認証システムの概略構成を示す図である。本実施形態の電子印鑑認証システムは、印鑑マークを管理する複数のシステム管理者１００A～システム管理者１００B（以下、単にシステム管理者１００とも称する）と、複数の社員１１０A～社員１１０B（以下、単に社員１１０とも称する）が利用するシステムであって、図１に示す様に印鑑マーク管理サーバ１０１A（以下、単に印鑑マーク管理サーバ１０１とも称する）と、社員端末１１１A（以下、単に社員端末１１１とも称する）とが、企業イントラネット等の通信網１２０A（以下、単に通信網１２０とも称する）を介して互いに接続されて構成されている。これにインターネット等を経由して他社の同様のシステム或いはクライアント端末が接続される。なおここでいう印鑑マークとは、視認性のある画像データであって、印鑑を押印する本人に第３者が成りすましていないかの検証（以下、単に本人認証とも称する）及び印鑑を押印された文書等のデジタルデータが改ざんされていないかの検証（以下、単に文書認証とも称する）を行う為の、印鑑やサイン等のイメージデザインの形状をとるマークを示すものとする。

【００２０】印鑑マーク管理サーバ１０１は、システム管理者１００が管理する企業イントラネットや企業間のネットワーク取引で本人認証や文書認証を行うマーク管理サーバである。印鑑マーク管理サーバ１０１は、社員１１０の要求に応じて、各自の本人認証に必要な情報を埋め込んだ印鑑マークを作成し、後述の印鑑マーク管理ＤＢに登録する。この時、印鑑マークのデザインは社員１１０が自由に作成できるが、不正な登録を防ぐ為に社員ＩＤ等で要求元の確認を行う。

【００２１】社員端末１１１は社員１１０が利用するマーク端末装置である。社員１１０は、社員端末１１１を使ってビジネスに必要な文書等を作成したり、システム管理者１００とデータのやり取りをしたりする。各自の印鑑マークは社員端末１１１等で管理される。所属等の情報変更時にはシステム管理者１００が印鑑マークの更新を行い、更新した印鑑マークを社員端末１１１に送信する。画面イメージ１１２は、印鑑マーク付きのデジタルデータを表示した時の画面表示例である。

【００２２】図２は本実施形態の印鑑マーク管理サーバ１０１の概略構成を示す図である。図２に示す様に本実施形態の印鑑マーク管理サーバ１０１は、印鑑マーク管理処理部２２１と、印鑑マーク公開鍵管理処理部２２２とを有している。

【００２３】印鑑マーク管理処理部２２１は、印鑑マークの新規登録または更新を要求するマーク登録要求を社員端末１１１から受信し、要求元の人物を認証する為の情報を秘密鍵で暗号化した本人認証情報を当該要求元の印影デザインに埋め込んで印鑑マークを作成し、前記作成した印鑑マークに前記本人認証情報を復号化する為の公開鍵を添付して要求元に配布するマーク管理処理部である。

【００２４】印鑑マーク公開鍵管理処理部２２２は、暗号化した本人認証情報を復号化する為の公開鍵を印鑑マーク公開鍵管理ＤＢ２１１に登録し、前記登録した公開鍵を各社員端末１１１に送信するマーク復号鍵管理処理部である。

【００２５】印鑑マーク管理サーバ１０１を印鑑マーク管理処理部２２１及び印鑑マーク公開鍵管理処理部２２２として機能させる為のプログラムは、ＣＤ－ＲＯＭ等の記録媒体に記録され磁気ディスク等に格納された後、メモリにロードされて実行されるものとする。なお前記プログラムを記録する媒体はＣＤ－ＲＯＭ以外の他の媒体でも良い。

【００２６】図２に示す様に本実施形態の印鑑マーク管理サーバ１０１は、表示装置２０１と、入力装置２０２と、通信網インタフェース２０３と、印鑑マーク管理ＤＢインタフェース２０４と、印鑑マーク公開鍵管理ＤＢインタフェース２０５と、印鑑マークログ管理ＤＢインタフェース２０６と、記憶装置２０７と、ＣＰＵ２０８と、メモリ２０９とがバス２００によって互いに接続されて構成されている。また外部記憶装置として印鑑マーク管理ＤＢ２１０、印鑑マーク公開鍵管理ＤＢ２１１及び印鑑マークログ管理ＤＢ２１２が接続されている。

【００２７】表示装置２０１は、印鑑マーク管理サーバ１０１を使用するシステム管理者１００にメッセージ等を表示する為に用いられるものであり、ＣＲＴや液晶ディスプレイ等で構成される。入力装置２０２は、印鑑マーク管理サーバ１０１を使用するシステム管理者１００がデータや命令等を入力する為に用いられるものであり、キーボードやマウス等で構成される。通信網インタフェース２０３は、通信網１２０を介して、社員端末１１１や他社の印鑑マーク管理サーバ１０１B等とデータのやり取りを行う為のインタフェースである。

【００２８】印鑑マーク管理ＤＢインタフェース２０４は、印鑑マーク管理ＤＢ２１０とデータのやり取りを行う為のインタフェースである。印鑑マーク管理ＤＢ２１０は、社員ＩＤ、印鑑ＩＤ、印影等といったデータを対応付けて管理するものであり、例えば図４の様なものである。

【００２９】印鑑マーク公開鍵管理ＤＢインタフェース２０５は、印鑑マーク公開鍵管理ＤＢ２１１とデータのやり取りを行う為のインタフェースである。印鑑マーク公開鍵管理ＤＢ２１１は、取引きのある企業の情報システム管理部署等の印鑑マーク管理者と本人認証用の公開鍵等といったデータを対応付けて管理するものであり、例えば図５の様なものである。

【００３０】印鑑マークログ管理ＤＢインタフェース２０６は、印鑑マークログ管理ＤＢ２１２とデータのやり取りを行う為のインタフェースである。印鑑マークログ管理ＤＢ２１２は、社員端末１１１でデジタルデータに印鑑マークを押印する時に該印鑑マークに埋め込む文書認証データを対応付けて管理するものであり、例えば図７の様なものである。

【００３１】記憶装置２０７は、印鑑マーク管理サーバ１０１等で使用されるプログラムやデータを永続的に記憶する為に用いられるものであり、ハードディスクやフロッピーディスク等で構成される。

【００３２】ＣＰＵ２０８は、印鑑マーク管理サーバ１０１を構成する各部を統括的に制御したり、様々な演算処理を行ったりする。メモリ２０９には、ＯＳ２２０や印鑑マーク管理処理部２２１、印鑑マーク公開鍵管理処理部２２２といった、ＣＰＵ２０８が上記の処理をする為に必要なプログラム等が一時的に格納される。ここでＯＳ２２０は、印鑑マーク管理サーバ１０１全体の制御を行う為にファイル管理やプロセス管理或いはデバイス管理といった機能を実現する為のプログラムである。

【００３３】印鑑マーク管理処理部２２１は、社員端末１１１から印鑑マーク登録／変更要求があった場合に第３者からの不正な要求でないかを確認する処理、登録すると判定した場合に、送付された印影デザインまたは印鑑マーク管理ＤＢ２１０で管理している印影デザインに本人情報を埋め込む処理、処理に基づいて印鑑マーク管理ＤＢ２１０を更新する処理、要求元に印鑑マークを送信する処理及び印鑑マーク押印時に送信されるログ情報を印鑑マークログ管理ＤＢ２１２に格納する処理を行う処理部である。

【００３４】また印鑑マーク管理ＤＢ２１０は、権限を有した者のみが更新できるものとする。なお印影デザインに埋め込む本人情報は図６の様なものである。画像データの中に特定の情報を埋め込む技術は、「電子透かし」として知られている。「電子透かし」の技術については日経エレクトロニクス１９９７年６８３号の１００ページから１０７ページに記載されている。人間の目では判別できない様に情報を埋め込む不可視透かしと、人間の目にも見える形で情報を埋め込む可視透かしがあり、不可視透かしの場合埋め込む情報量に限界があると言われている。印鑑マークの場合、印鑑イメージが象徴する意味が分かる範囲、つまりそのマークが何を表すかが分かる範囲であれば、多少デザインを変更しても支障がないので、図８の様に可視透かしと不可視透かしを組み合わせて、ある程度多くの情報を埋め込むことができる。

【００３５】印鑑マーク公開鍵管理処理部２２２は、社外のデジタル文書に押印された印鑑マークの送り手の確認、つまり本人認証を行う為に必要な公開鍵を印鑑マーク公開鍵管理ＤＢ２１１に登録・管理する処理、新しい公開鍵が印鑑マーク公開鍵管理ＤＢ２１１に登録されたら社員端末１１１等に接続している公開鍵ＤＢに該公開鍵を送信する処理、及び公開鍵の送信要求があった場合には要求元に該公開鍵を送信する処理を行う処理部である。なお社外から公開鍵を受け取る場合は、企業のシステム管理者１００に第３者が成りすますことを防止する為に、発信元の身元確認を行った上でＦＤ等に格納した公開鍵を受け取るものとする。

【００３６】図３は本実施形態の社員端末１１１の概略構成を示す図である。図３に示す様に本実施形態の社員端末１１１は、印鑑マーク登録処理部３１２と、印鑑マーク押印処理部３１３と、印鑑マーク認証処理部３１４と、公開鍵格納処理部３１５とを有している。

【００３７】印鑑マーク登録処理部３１２は、印鑑マークの新規登録または更新を要求するマーク登録要求を印鑑マーク管理サーバ１０１に送信し、要求元の人物を認証する為の情報を秘密鍵で暗号化した本人認証情報を当該要求元の印影デザインに埋め込んで作成した印鑑マークを印鑑マーク管理サーバ１０１から受け取るマーク登録処理部である。

【００３８】印鑑マーク押印処理部３１３は、印鑑マークが付加される文書の特徴情報を含む文書認証情報と押印通算番号とをユーザ固有の秘密鍵で暗号化し、本人認証情報が埋め込まれた印鑑マークに前記暗号化された文書認証情報及び押印通算番号を埋め込み、前記文書の選択された位置に前記印鑑マークを付加するマーク付加処理部である。

【００３９】印鑑マーク認証処理部３１４は、文書に付加された印鑑マークから本人認証情報を抽出し、その本人認証情報を復号化する為に添付された公開鍵が公開鍵ＤＢ３０９に格納されている公開鍵と合致するかどうか照合し、前記公開鍵が合致している場合には前記印鑑マークから抽出した本人認証情報を前記公開鍵で復号化して本人認証情報を表示し、合致していない場合にはエラーメッセージを表示する本人認証処理と、文書に付加された印鑑マークから文書認証情報を抽出して公開鍵により復号化し、印鑑マークが付加されている文書から特徴

情報を抽出し、前記文書から抽出した特徴情報と印鑑マークから抽出した文書認証情報中の特徴情報とを比較照合し、特徴情報が合致している場合には前記文書認証情報の表示を行い、合致していない場合にはエラーメッセージを表示するデータ認証処理とを行うマーク認証処理部である。公開鍵格納処理部３１５は、本人認証情報を復号化する為の公開鍵を印鑑マーク管理サーバ１０１から受信し、前記公開鍵を公開鍵ＤＢ３０９に格納する復号鍵格納処理部である。

【００４０】社員端末１１１を印鑑マーク登録処理部３１２、印鑑マーク押印処理部３１３、印鑑マーク認証処理部３１４及び公開鍵格納処理部３１５として機能させる為のプログラムは、ＣＤ－ＲＯＭ等の記録媒体に記録され磁気ディスク等に格納された後、メモリにロードされて実行されるものとする。なお前記プログラムを記録する媒体はＣＤ－ＲＯＭ以外の他の媒体でも良い。

【００４１】図３に示す様に本実施形態の社員端末１１１は、表示装置３０１と、入力装置３０２と、通信網インタフェース３０３と、公開鍵ＤＢインタフェース３０４と、記憶装置３０５と、ＣＰＵ３０６と、メモリ３０７とがバス３００によって互いに接続されて構成されている。また印影デザインとして従来実社会で使用している印鑑のデザインを利用する場合には、イメージスキャナ３０８を接続して使用したいデザインをビットマップ等で読み込んだ後に編集できる様にする。

【００４２】表示装置３０１は、社員端末１１１を使用する社員１１０にメッセージ等を表示する為に用いられるものであり、ＣＲＴや液晶ディスプレイ等で構成されている。入力装置３０２は、社員端末１１１を使用する社員１１０がデータや命令等を入力する為に用いられるものであり、キーボードやマウス等で構成される。通信網インタフェース３０３は、通信網１２０を介して、印鑑マーク管理サーバ１０１や社員端末１１１B等とデータのやり取りを行う為のインタフェースである。

【００４３】公開鍵ＤＢインタフェース３０４は、公開鍵ＤＢ３０９がある場合にデータのやり取りを行う為のインタフェースである。記憶装置３０５は、社員端末１１１等で使用されるプログラムやデータを永続的に記憶する為に用いられるものであり、ハードディスクやフロッピーディスク等で構成される。

【００４４】ＣＰＵ３０６は、社員端末１１１を構成する各部を統括的に制御したり、様々な演算処理を行ったりする。メモリ３０７には、ＯＳ３１０や、グループウェアシステム等３１１、印鑑マーク認証処理部３１４、印鑑マーク情報記憶部３１６といった、ＣＰＵ３０６が上記の処理をする為に必要なプログラム等が一時的に格納される。ここでＯＳ３１０は、社員端末１１１全体の制御を行う為にファイル管理やプロセス管理或いはデバイス管理といった機能を実現する為のプログラムである。グループウェアシステム等３１１は、社員端末１１１が社内外とデジタルデータをやり取りし、必要なデータを表示する為のシステムで、デジタルデータに押印された認証情報を扱う為に、印鑑マーク認証処理部３１４とのインタフェースを持つ。なおこのグループウェアシステム等３１１の部分は、デジタルデータをハンドリングするアプリケーションシステムであれば、どの様なものでも良く、特にグループウェアシステムに限定するものではない。また、直接印鑑マーク認証処理部３１４を個別アプリケーションシステムとしてＯＳ３１０上で動かす場合もある。

【００４５】印鑑マーク登録処理部３１２は、印鑑マーク登録の為の印影デザインを作成する処理、印鑑マーク管理サーバ１０１に印鑑マーク登録要求を送信する処理及び印鑑マーク管理サーバ１０１から送信された印鑑マークを受信する処理を行う。

【００４６】印鑑マーク押印処理部３１３は、社員１１０が社員端末１１１でデジタルデータに電子印鑑を押印する為の処理で、必要なデジタルデータを表示し、社員ＩＤに対応するパスワードが入力されたら、該社員ＩＤに対応する印鑑マークを呼び出す処理、選択された文書認証情報と印鑑マークの押印通算番号等の押印時情報を固有の秘密鍵で暗号化したものを印鑑マークの特定のブロックに埋め込む処理及び文書の指定された位置に印鑑マークを押印する処理等を行う。

【００４７】印鑑マーク認証処理部３１４は、社員１１０が社員端末１１１で受信したデジタルデータの送り手や内容の認証を行う為の処理部である。必要なデジタルデータを表示し、選択された認証項目に対応して、印鑑マークに埋め込まれた本人認証情報を予め印鑑マーク管理サーバ１０１より配布された公開鍵で復号化して表示する本人認証処理、印鑑マークに埋め込まれた文書認証情報を印鑑マークに添付された公開鍵で復号化して表示する文書認証処理、前記公開鍵で復号化できない場合にエラーメッセージを表示する処理及び表示したデジタルデータの有効期限やファイル名等の情報をチェックし、無効と判断される場合は印影を無効なデザインに変形させる処理等を行う。

【００４８】印鑑マーク情報記憶部３１６は、印鑑マーク認証処理部３１４によって社員端末１１１で呼び出した印鑑マークや公開鍵を一時的に格納するものである。なお企業間でネットワーク取引を行う等、本人認証情報の確認の為に必要な公開鍵が複数必要な場合は、公開鍵ＤＢ３０９を社員端末１１１或いは通信網１２０に接続し、印鑑マーク公開鍵管理ＤＢ２１１から必要な公開鍵を公開鍵ＤＢインタフェース３０４に送信し、社員端末１１１から参照できる様にする。また企業イントラネット内でのみ印鑑マークを用いる場合は、予め社員端末１１１に公開鍵を持たせておいても良く、公開鍵の格納方法は限定しない。

【００４９】図４は本実施形態の印鑑マーク管理ＤＢ２

１０のデータ例を示す図である。社員ＩＤ４０１、印鑑ＩＤ４０２、氏名４０３、メールアドレス４０４、所属・役職他の情報４０５、印影データ４０６等を一定の表記基準に基づいて表記を統一して格納する。新しい印鑑マークを登録したり、既存の印鑑マークの所属・役職他の情報４０５を変更した際等に印鑑マーク管理ＤＢ２１０を更新する。

【００５０】図５は本実施形態の印鑑マーク公開鍵管理ＤＢ２１１のデータ例を示す図である。データ番号５０１、印鑑マーク管理者５０２、管理者アドレス５０３、公開鍵データ５０４等を一定の表記基準に基づいて表記を統一して格納する。印鑑マーク公開鍵管理ＤＢ２１１は、本人認証の為の公開鍵データ５０４を管理するＤＢであり、新たに印鑑マークを利用する企業が増えたり、公開鍵データ５０４の変更があった際等に印鑑マーク公開鍵管理ＤＢ２１１を更新する。なお予め公開鍵データ５０４の有効期限等が設定されている場合はそのデータも管理する。

【００５１】図６は本実施形態の本人認証データの例を示す図である。図６では印鑑マーク管理サーバ１０１において印鑑マーク管理処理部２２１が、社員１１０の要求に応じて印影に本人認証情報を埋め込む際の本人認証データの例を表している。印鑑ＩＤ６０１、氏名６０２、メールアドレス６０３、所属・役職他６０４等を、印鑑マーク管理サーバ１０１の印鑑マーク管理処理部２２１によって印鑑マーク管理サーバ１０１で管理する秘密鍵で暗号化して印鑑マークのエンティティとして埋め込む。埋め込む際には、例えば図８の印影イメージ８０２の様に、印影の氏名部分に不可視透かしで埋め込み、可視透かしの形で会社名を埋め込む。つまり、予め印影の中を２つ以上のブロックに区分し、特定のブロックに本人認証情報を埋め込む。なお社印の様な印鑑においては、押印の責任部署を本人認証情報として用いる場合もある。

【００５２】図７は本実施形態の文書認証データの例を示す図である。図７では社員端末１１１において社員１１０がデジタルデータに印鑑マークを押印する際に文書認証情報として埋め込まれる文書認証データの例を表している。社員端末１１１の印鑑マーク押印処理部３１３は、印鑑ＩＤ７０１、印鑑マーク押印通算ＮＯ．７０２、作成日時７０３、有効期限７０４、ファイル名７０５、端末ＩＤ７０６、押印したいデジタルデータの特徴情報７０７等を印鑑マーク押印処理部３１３が管理する秘密鍵によって社員端末１１１で暗号化して印鑑マークのエンティティとして埋め込む。例えば図８の印影イメージ８０３の様に、本人認証情報を埋め込んだブロック以外の印影の周辺部分に文書認証情報の埋め込みを行う。デジタルデータの特徴情報７０７としては、文字データのコードを数値とみなして加算した、いわゆるチェックサムと呼ばれるものやデジタルデータの内容の圧縮文等を用いる。

【００５３】また図７は印鑑マークログ管理ＤＢ２１２のデータ例でもある。社員端末１１１の印鑑マーク押印処理部３１３によって、図７の様なデータを押印時のログ情報として印鑑マーク管理サーバ１０１に送信し、印鑑マーク管理処理部２２１によって該ログ情報を印鑑マークログ管理ＤＢ２１２に格納する。なお本人認証及び文書認証に必要なデータは、図６及び図７の例に限らず、ＩＳＯ９００１の認証を取得する際の電子データの記録情報として必要な情報を満たすものとする。

【００５４】図８は本実施形態の印影及び印鑑マークのイメージ例を示す図である。例えば印影イメージ８０１の様な印影に、本人認証情報を埋め込む。この時、予め印影の中を２つ以上のブロックに区分し、各々特定のブロックに本人認証情報や文書認証情報を埋め込むことにする。例えば、印影イメージ８０２の様に氏名部分と可視透かしの会社名部分に、本人認証情報を埋め込み、印影イメージ８０３の様な印影の周辺部分に文書認証情報を埋め込むといったブロック区分を行い、社員端末１１１の印鑑マーク認証処理部３１４で認証情報を復号化する際には、対応するブロックから埋め込まれた情報が自動的に抽出される様にする。なお印影イメージ８０１では、印影デザイン例として個人の認め印のデザインを用いたが、日付入りの職印やサイン等のデザインでも良いし、また社印として用いる際には企業名等でも良く、印影イメージ８０１の印影デザイン例に限定するものではない。但し単なるイメージデザインと異なり、認証情報が埋め込まれていると感じられる様な信頼感を与える印影デザインであることが重要である。

【００５５】次に本実施形態の電子印鑑認証システムの動作について説明する。図９は本実施形態の初期画面のイメージ例を示す図である。図９では社員端末１１１によって表示される電子印鑑認証システムの初期画面イメージ例を表している。初期画面９００は、必要なデジタル文書等を表示するデジタルデータ表示エリア９０１と、印鑑マークの機能アイコンが並ぶ印鑑マーク機能表示エリア９０２と、ＯＫ、キャンセル、ファイルといった基本機能のアイコンが並ぶ基本機能表示エリア９０３により構成される。但し初期画面９００は各エリアの配置例であり、この配置に限定するものではない。

【００５６】図１０は本実施形態の印鑑マーク登録処理の処理手順を示すフローチャートである。図１０では社員端末１１１と印鑑マーク管理サーバ１０１との間で印鑑マークの登録を行う処理フローを表している。まず社員１１０が、図９の様な初期画面９００の印鑑マーク機能表示エリア９０２の登録ボタンをクリックすると、印鑑マーク登録処理部３１２は、印鑑マークの登録要求を印鑑マーク管理サーバ１０１に送信する（ステップ１００１）。印鑑マーク登録要求を受信した印鑑マーク管理サーバ１０１は、印鑑マーク管理処理部２２１によっ

て、登録要求元の社員ＩＤ４０１を元に印鑑マーク管理ＤＢ２１０から要求元のメールアドレス４０４を読み出し、要求元のメールアドレス４０４に印鑑マーク要求／変更の確認依頼を送信する（ステップ１００２及びステップ１００３）。確認依頼を受信した社員端末１１１の印鑑マーク登録処理部３１２は、イメージスキャナ等を用いて作成した、登録或いは変更したい印影デザインを印鑑マークの要求確認結果と共に印鑑マーク管理サーバ１０１に送信する（ステップ１００４及びステップ１００５）。印影と印鑑マークの要求確認結果を受信した印鑑マーク管理サーバ１０１は、印鑑マーク管理処理部２２１を用いて、印鑑マーク管理サーバ１０１で管理する当該サーバの秘密鍵で本人認証情報を暗号化し、これを受信した印影デザインに埋め込んで印鑑マークを作成する（ステップ１００８）。印鑑マーク管理ＤＢ２１０内の登録或いは変更した印鑑マークの情報を更新した後（ステップ１００９）、その本人認証情報を復号する為の公開鍵と共に前記作成した印鑑マークを要求元の社員１１０にＦＤ等で配布する（ステップ１０１０）。社員１１０は、配布された印鑑マークを社員端末１１１に格納する（ステップ１０１１及びステップ１０１２）。

【００５７】図１１は本実施形態の印鑑マーク押印処理の処理手順を示すフローチャートである。図１１では社員端末１１１において文書認証情報を埋め込んだ印鑑マークを文書に押印する処理フローを表している。図１２は本実施形態の図１１の処理フローに対応する処理画面のイメージを示す図である。この図１１及び図１２と前述の図９を用いて、上記処理フローを説明する。まず社員１１０が、押印したい文書データ等を基本機能表示エリア９０３にあるファイルボタンにより選択し、デジタルデータ表示エリア９０１に表示する（ステップ１１０１）。印鑑マーク機能表示エリア９０２の印鑑マークの呼出ボタンをクリックすると、印鑑マーク押印処理部３１３によって、図１２の処理画面イメージ１２０１の様な社員ＩＤ４０１とパスワードの入力欄が表示される（ステップ１１０２及びステップ１１０３）。印鑑マーク押印処理部３１３は、入力されたパスワードと予め社員端末１１１に格納されているパスワードとを照合し、合致しなかった場合はエラーメッセージを表示し、合致した場合は印鑑マーク欄に印鑑マークを表示する（ステップ１１０４～ステップ１１０６）。次に文書情報の埋め込みボタンをクリックすると、図１２の処理画面イメージ１２０２の様に、印鑑マーク押印処理部３１３によって文書認証情報の項目欄を表示する（ステップ１１０７及びステップ１１０８）。必要な項目を選択してＯＫをクリックすると印鑑マーク押印処理部３１３は、選択された文書情報と押印通算番号を社員毎に予め決められた各社員に固有の秘密鍵で暗号化して印鑑マークに埋め込み、また、その復号化に必要な公開鍵を添付して印鑑マーク欄に該印鑑マークを表示する（ステップ１１０９～ステップ１１１３）。押印位置を選択して印鑑マーク機能表示エリア９０２の押印ボタンをクリックすると印鑑マーク押印処理部３１３は、印鑑マークを文書の設定された位置に押印する（ステップ１１１４～ステップ１１１６）。なお文書認証情報の復号の為に必要な社員固有の公開鍵は、印鑑マークに添付せずに本人認証時に取得するものとしても良い。

【００５８】図１３は本実施形態の本人認証処理の処理手順を示すフローチャートである。図１４は本実施形態の図１３の処理フローに対応する処理画面のイメージ例を示す図である。まず社員端末１１１で図１４の処理画面イメージ１４０１の様に印鑑マークが貼り付けられたデジタルデータを表示し、社員１１０が印鑑マークの認証ボタンをクリックすると、印鑑マーク認証処理部３１４は印鑑マークの認証項目欄を表示する（ステップ１３０１及びステップ１３０２）。図１４の処理画面イメージ１４０２の様に社員１１０が印鑑マークの本人認証項目をクリックすると、印鑑マーク認証処理部３１４は、該印鑑マークから本人認証情報を抽出する（ステップ１３０３）。抽出した本人認証情報を復号化する為の公開鍵が、社員端末１１１或いは公開鍵ＤＢ３０９に格納してある公開鍵と合致するかどうか照合する（ステップ１３０５）。復号化する為の公開鍵が合致した場合に印鑑マーク認証処理部３１４は、該印鑑マークから抽出した本人認証情報を復号化して、内容を確認できる様に図１４の処理画面イメージ１４０３の様に本人認証情報を表示し（ステップ１３０６）、合致しなければエラーメッセージを表示する（ステップ１３０７）。更に、エラーメッセージを表示した場合は、印影を消す、印影に×を付ける等、印鑑マークを無効なデザインに変形する（ステップ１３０８）。また本人認証情報として表示された内容を本人に確認したい場合は、本人認証情報の中のメールアドレス宛に確認依頼のメールを送信する。なお本人認証結果の表示方法は、図１４の処理画面イメージ例に限定されるものではなく、例えばエラーメッセージは音声等によって表現しても良い。

【００５９】図１５は本実施形態の文書認証処理の処理手順を示すフローチャートである。なお文書認証処理フローの最初の工程で、本人認証処理フローと同じ部分、図１３でいうとステップ１３０１及びステップ１３０２に相当する部分は省略した。図１６は本実施形態の図１５の処理フローに対応する処理画面のイメージ例を示す図である。まず社員１１０が、社員端末１１１で図１６の処理画面イメージ１６０１の様に印鑑マークの文書認証項目をクリックする（ステップ１５０１）。印鑑マーク認証処理部３１４は、該印鑑マークから文書情報の復号化に必要な公開鍵と文書認証情報を抽出し、文書認証情報を復号化する（ステップ１５０２～ステップ１５０４）。次に該印鑑マークが押印されている文書等のデジタルデータから特徴情報を抽出し、該印鑑マークから抽

出した文書認証情報の中の特徴情報７０７と比較照合する（ステップ１５０５及びステップ１５０６）。この結果、合致しなかった場合は、文書等のデジタルデータが作成時点のものと異なることになるので、「このデータは変更されています」等のエラーメッセージを表示し、かつ印影を消す、印影に×を付ける等、印鑑マークを無効なデザインに変形する（ステップ１５０７及びステップ１５０８）。特徴情報７０７が合致した場合は更に有効期限等の情報を確認し、ＯＫであれば図１６のステップ処理画面イメージ１６０２の様に確認の為の文書情報の表示を行い（ステップ１５０９及びステップ１５１０）、有効期限７０４が切れている等の場合には、印影を消す、印影に×を付ける等、印鑑マークを無効なデザインに変形する（ステップ１５０８）。なお文書認証結果の表示方法は、図１６の処理画面イメージ例に限定されるものではなく、例えばエラーメッセージの表示は音等でも良い。

【００６０】印鑑マークの第３者による不正押印を防ぐ為にパスワードを用いているが、よりセキュリティを高める為に、例えばパスワードをＩＤカードで管理し、使用する時には印鑑マーク認証処理部３１４によってＩＤカードからパスワードを読み取る様にしても良い。この時、パスワードを予め暗号化しておくとよりセキュリティが高くなる。

【００６１】また本人認証情報のみが埋め込まれた他者の印鑑マークを不正入手し、自分の秘密鍵で文書情報を該印鑑マークに埋め込み、不正使用する等への対応策としては、例えば印鑑マークの押印通算ＮＯ．７０２を利用する。社員端末１１１で文書認証情報を埋め込んだ印鑑マークを押印時に、押印通算ＮＯ．７０２をログ情報として自動的に印鑑マーク管理サーバ１０１に送信し、印鑑マークログ管理ＤＢ２１２でログ情報を管理することで前述の様な不正が行われた際にチェックすることができる。

【００６２】以上、本発明の実施形態について企業イントラネット及び企業間ネットワークの例を用いて説明したが、本発明はこの実施形態に限定されるものではない。例えば個人がネットワーク上で電子商取引を行う際に作成する注文書の様な、ネットワーク上でやり取りする一般的なデジタルデータに適用することも可能である。また従来印鑑証明を発行していた自治体が印鑑マーク管理機関になり、実印の印鑑登録時に、印鑑マークを申請した人に対してＦＤ等で本人認証情報を埋め込んだ印鑑マークと印鑑マーク認証処理部３１４を配布する方法も考えられる。

【００６３】以上説明した様に本実施形態の電子マーク認証システムによれば、本人認証情報及びデジタルデータ認証情報を埋め込んで作成したマークをデジタルデータに付加し、マーク中の認証情報を用いて当該デジタルデータの認証を行うので、ネットワーク上でデジタルデータを送受信する際の本人認証及びデータ認証を実現することが可能である。

【００６４】

【発明の効果】本発明によれば本人認証情報及びデジタルデータ認証情報を埋め込んで作成したマークをデジタルデータに付加し、マーク中の認証情報を用いて当該デジタルデータの認証を行うので、ネットワーク上でデジタルデータを送受信する際の本人認証及びデータ認証を実現することが可能である。

【図面の簡単な説明】

【図１】本実施形態の電子印鑑認証システムの概略構成を示す図である。

【図２】本実施形態の印鑑マーク管理サーバ１０１の概略構成を示す図である。

【図３】本実施形態の社員端末１１１の概略構成を示す図である。

【図４】本実施形態の印鑑マーク管理ＤＢ２１０のデータ例を示す図である。

【図５】本実施形態の印鑑マーク公開鍵管理ＤＢ２１１のデータ例を示す図である。

【図６】本実施形態の本人認証データの例を示す図である。

【図７】本実施形態の文書認証データの例を示す図である。

【図８】本実施形態の印影及び印鑑マークのイメージ例を示す図である。

【図９】本実施形態の初期画面のイメージ例を示す図である。

【図１０】本実施形態の印鑑マーク登録処理の処理手順を示すフローチャートである。

【図１１】本実施形態の印鑑マーク押印処理の処理手順を示すフローチャートである。

【図１２】本実施形態の図１１の処理フローに対応する処理画面のイメージを示す図である。

【図１３】本実施形態の本人認証処理の処理手順を示すフローチャートである。

【図１４】本実施形態の図１３の処理フローに対応する処理画面のイメージ例を示す図である。

【図１５】本実施形態の文書認証処理の処理手順を示すフローチャートである。

【図１６】本実施形態の図１５の処理フローに対応する処理画面のイメージ例を示す図である。

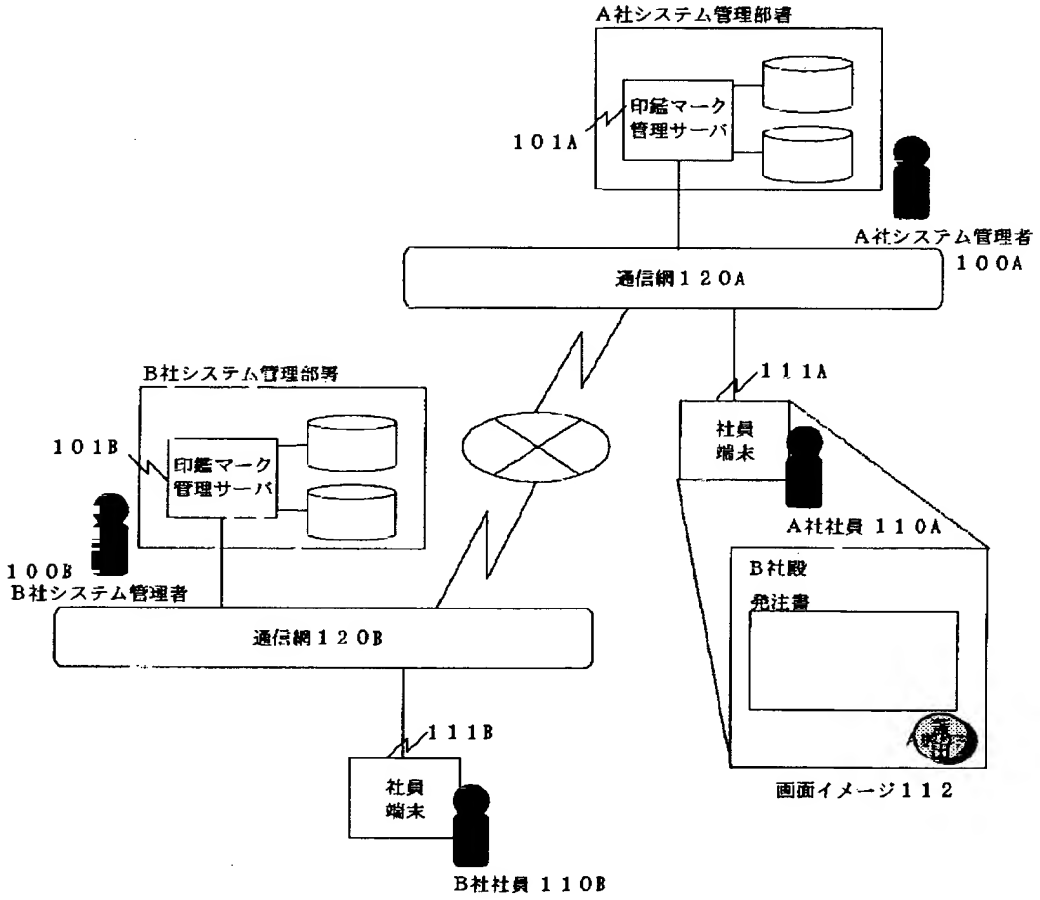
【符号の説明】

１００…システム管理者、１０１…印鑑マーク管理サーバ、１１０…社員、１１１…社員端末、１１２…画面イメージ、１２０…通信網、２００…バス、２０１…表示装置、２０２…入力装置、２０３…通信網インタフェース、２０４…印鑑マーク管理ＤＢインタフェース、２０５…印鑑マーク公開鍵管理ＤＢインタフェース、２０６…印鑑マークログ管理ＤＢインタフェース、２０７…記

憶装置、２０８…ＣＰＵ、２０９…メモリ、２１０…印鑑マーク管理ＤＢ、２１１…印鑑マーク公開鍵管理ＤＢ、２１２…印鑑マークログ管理ＤＢ、２２０…ＯＳ、２２１…印鑑マーク管理処理部、２２２…印鑑マーク公開鍵管理処理部、３００…バス、３０１…表示装置、３０２…入力装置、３０３…通信網インタフェース、３０４…公開鍵ＤＢインタフェース、３０５…記憶装置、３０６…ＣＰＵ、３０７…メモリ、３０８…イメージスキャナ、３０９…公開鍵ＤＢ、３１０…ＯＳ、３１１…グループウェアシステム等、３１６…印鑑マーク情報記憶部、３１２…印鑑マーク登録処理部、３１３…印鑑マーク押印処理部、３１４…印鑑マーク認証処理部、３１５…公開鍵格納処理部、４０１…社員ＩＤ、４０２…印鑑ＩＤ、４０３…氏名、４０４…メールアドレス、４０５…所属・役職他の情報、４０６…印影データ、５０１…データ番号、５０２…印鑑マーク管理者、５０３…管理者アドレス、５０４…公開鍵データ、６０１…印鑑ＩＤ、６０２…氏名、６０３…メールアドレス、６０４…所属・役職他、７０１…印鑑ＩＤ、７０２…通算ＮＯ．、７０３…作成日時、７０４…有効期限、７０５…ファイル名、７０６…端末ＩＤ、７０７…特徴情報、８０１～８０３…印影イメージ、９００…初期画面、９０１…デジタルデータ表示エリア、９０２…印鑑マーク機能表示エリア、９０３…基本機能表示エリア、１２０１～１２０３…処理画面イメージ、１４０１～１４０３…処理画面イメージ、１６０１及び１６０２…処理画面イメージ。

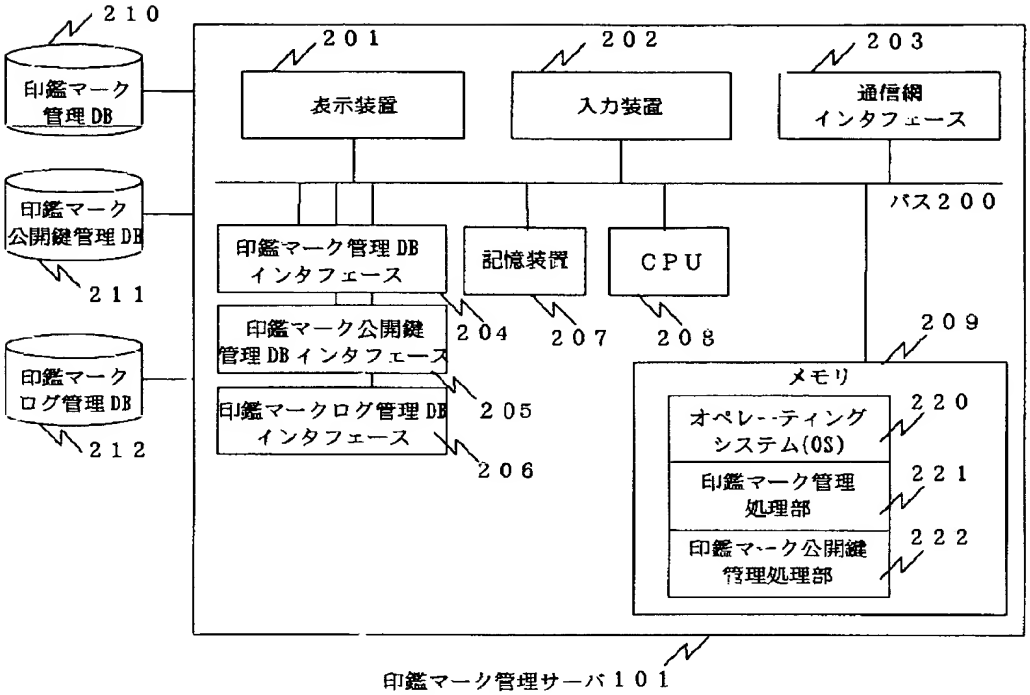
【図１】

図１



【図2】

図2




【図4】

図4

| 401 社員ID | 402 印鑑ID | 403 氏名 | 404 メールアドレス | 405 所属・役職他 | 406 印影 |
|---|---|---|---|---|---|
| D001101117 | A00123 | 相川太郎 | Aikawa@aa.co.jp | ○○事業部 事業部長 | 相川 |
| A035410506 | A00124 | 藍田次郎 | Aida@aa.co.jp | ○○事業部 課長 | 藍田 |
| H001100402 | - | 愛野三郎 | Aino@aa.co.jp | ○○事業部 担当 | - |
| | | | | | |

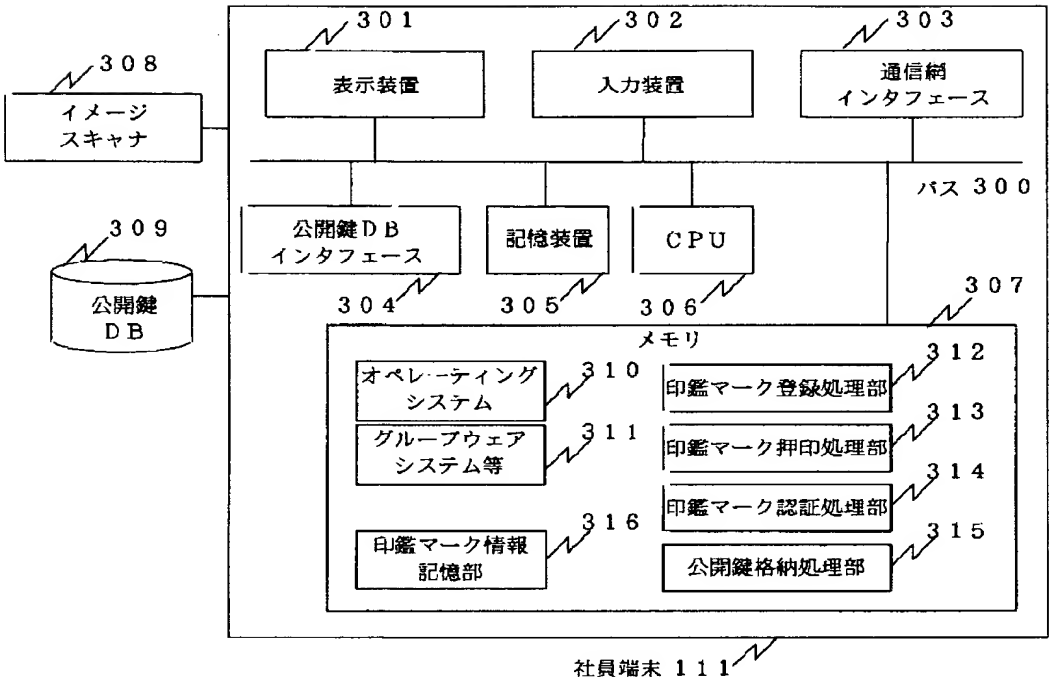
【図6】

図6

| 601 印鑑ID. | 602 氏名 | 603 メールアドレス | 604 所属・役職他 |
|---|---|---|---|
| A00123 | 相川太郎 | Aikawa@aa.co.jp | ○○事業部 事業部長 |

【図3】

図3




【図5】

図5

| 501 NO | 502 印鑑マーク管理者 | 503 管理者アドレス | 504 公開鍵 |
|---|---|---|---|
| 1 | A社印鑑マーク管理 | iz@aa.co.jp | pw＊＊＊＊gl＊＊＊＊＊qqm＊ |
| 2 | B社印鑑マーク管理 | im@bb.co.jp | ＊ajk＊＊yu＊＊＊＊＊aqz＊r |
| | | | |

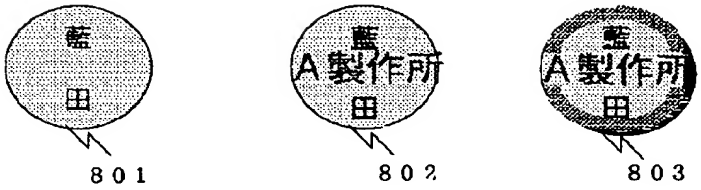
【図7】

図7

| 701 印鑑ID. | 702 通算NO. | 703 作成日時 | 704 有効期限 | 705 ファイル名 | 706 端末ID | 707 データの特徴情報 |
|---|---|---|---|---|---|---|
| A00123 | 000089 | 1998.7.7 | 1998.12.31 | 158.2＊＊/＊＊.doc | PC792 | ＊＊＊＊＊＊＊＊ |

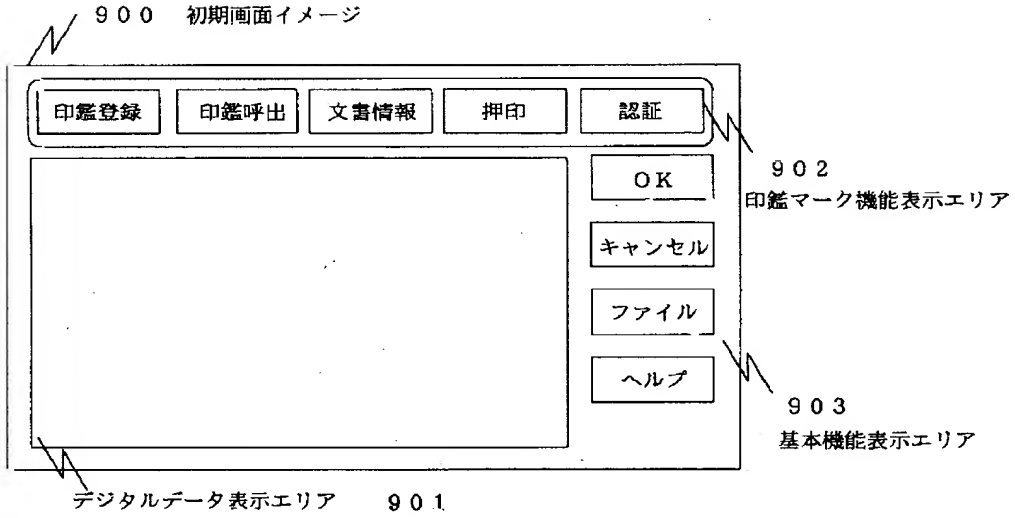
【図8】

図8


藍
田
801
藍
A製作所
田
802
藍
A製作所
田
803

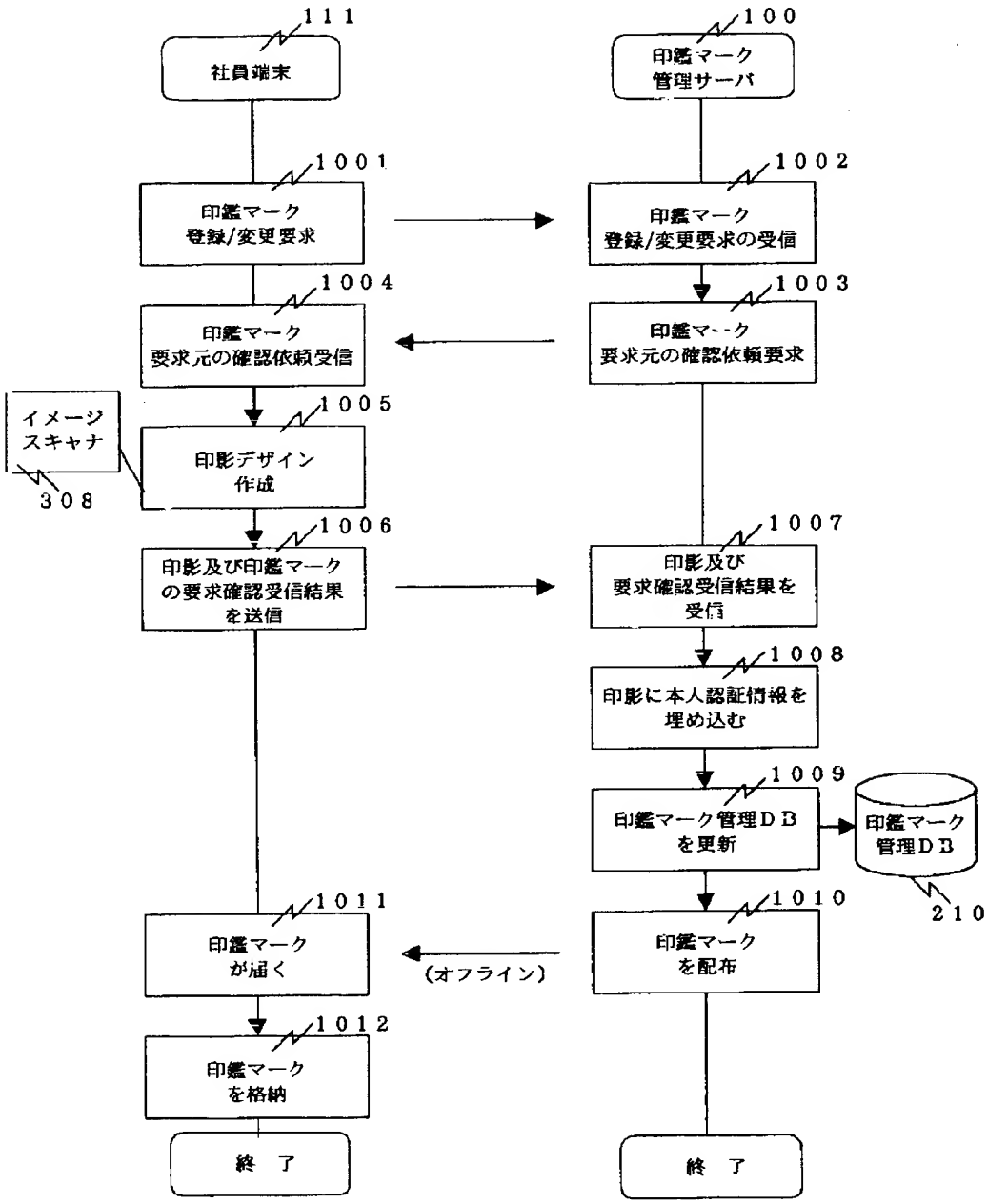
【図9】

図9


900 初期画面イメージ
印鑑登録
印鑑呼出
文書情報
押印
認証
OK
キャンセル
ファイル
ヘルプ
902
印鑑マーク機能表示エリア
903
基本機能表示エリア
デジタルデータ表示エリア 901

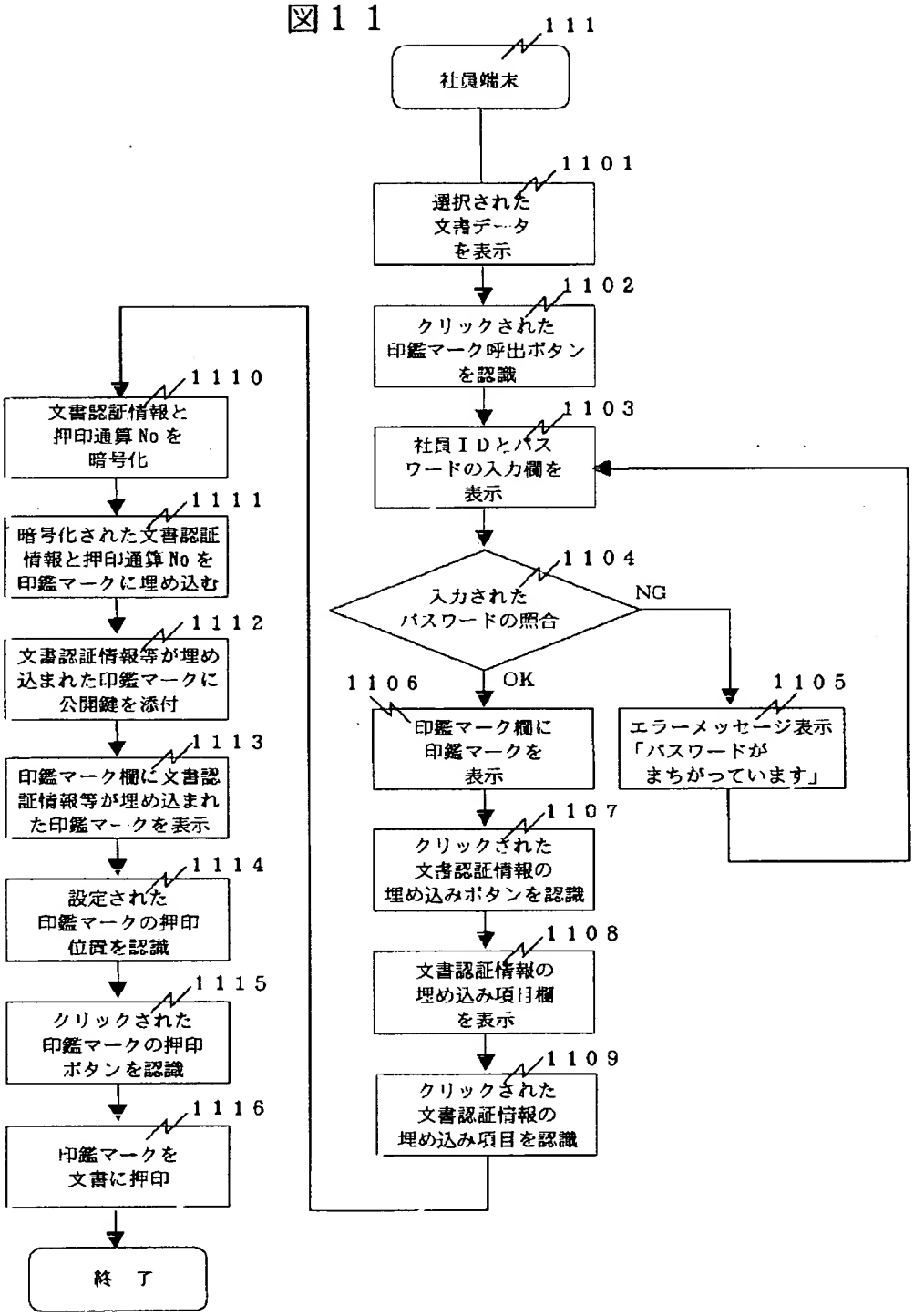
【図10】

図10


111
社員端末
100
印鑑マーク
管理サーバ
1001
印鑑マーク
登録/変更要求
1002
印鑑マーク
登録/変更要求の受信
1004
印鑑マーク
要求元の確認依頼受信
1003
印鑑マーク
要求元の確認依頼要求
イメージ
スキャナ
308
1005
印影デザイン
作成
1006
印影及び印鑑マーク
の要求確認受信結果
を送信
1007
印影及び
要求確認受信結果を
受信
1008
印影に本人認証情報を
埋め込む
1009
印鑑マーク管理DB
を更新
印鑑マーク
管理DB
210
1011
印鑑マーク
が届く
(オフライン)
1010
印鑑マーク
を配布
1012
印鑑マーク
を格納
終 了
終 了

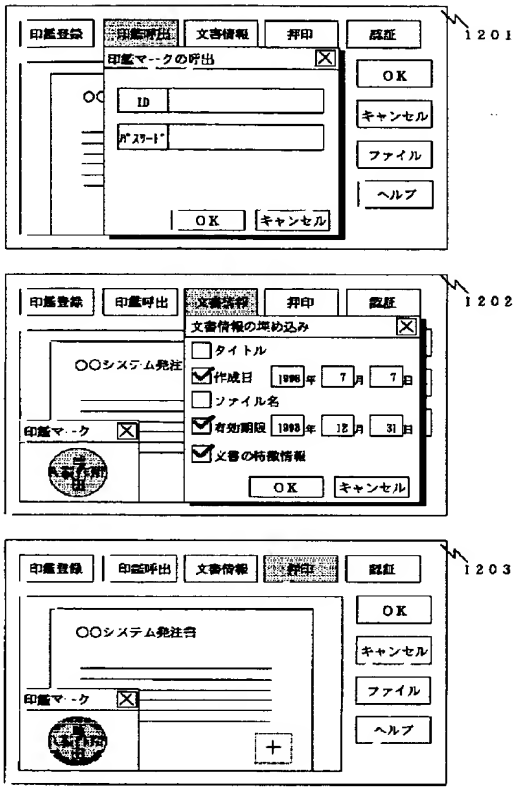
【図11】

図11


111
社員端末
1101
選択された
文書データ
を表示
1102
クリックされた
印鑑マーク呼出ボタン
を認識
1103
社員ＩＤとパス
ワードの入力欄を
表示
1104
入力された
パスワードの照合
NG
OK
1105
エラーメッセージ表示
「パスワードが
まちがっています」
1106
印鑑マーク欄に
印鑑マークを
表示
1107
クリックされた
文書認証情報の
埋め込みボタンを認識
1108
文書認証情報の
埋め込み項目欄
を表示
1109
クリックされた
文書認証情報の
埋め込み項目を認識
1110
文書認証情報と
押印通算Noを
暗号化
1111
暗号化された文書認証
情報と押印通算Noを
印鑑マークに埋め込む
1112
文書認証情報等が埋め
込まれた印鑑マークに
公開鍵を添付
1113
印鑑マーク欄に文書認
証情報等が埋め込まれ
た印鑑マークを表示
1114
設定された
印鑑マークの押印
位置を認識
1115
クリックされた
印鑑マークの押印
ボタンを認識
1116
印鑑マークを
文書に押印
終　了

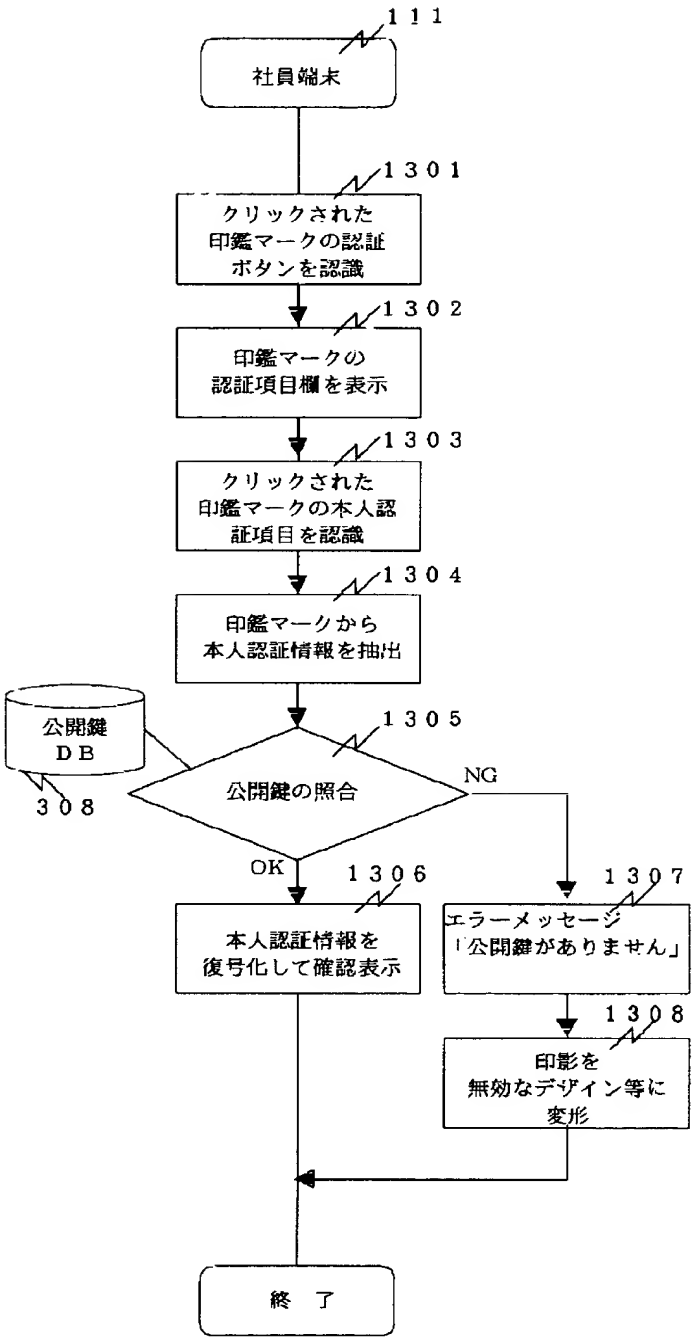
【図12】

図12



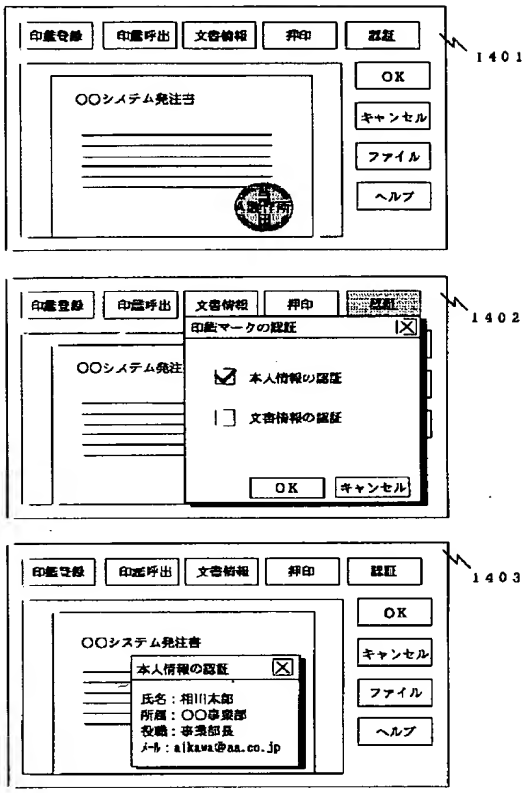

【図13】

図13



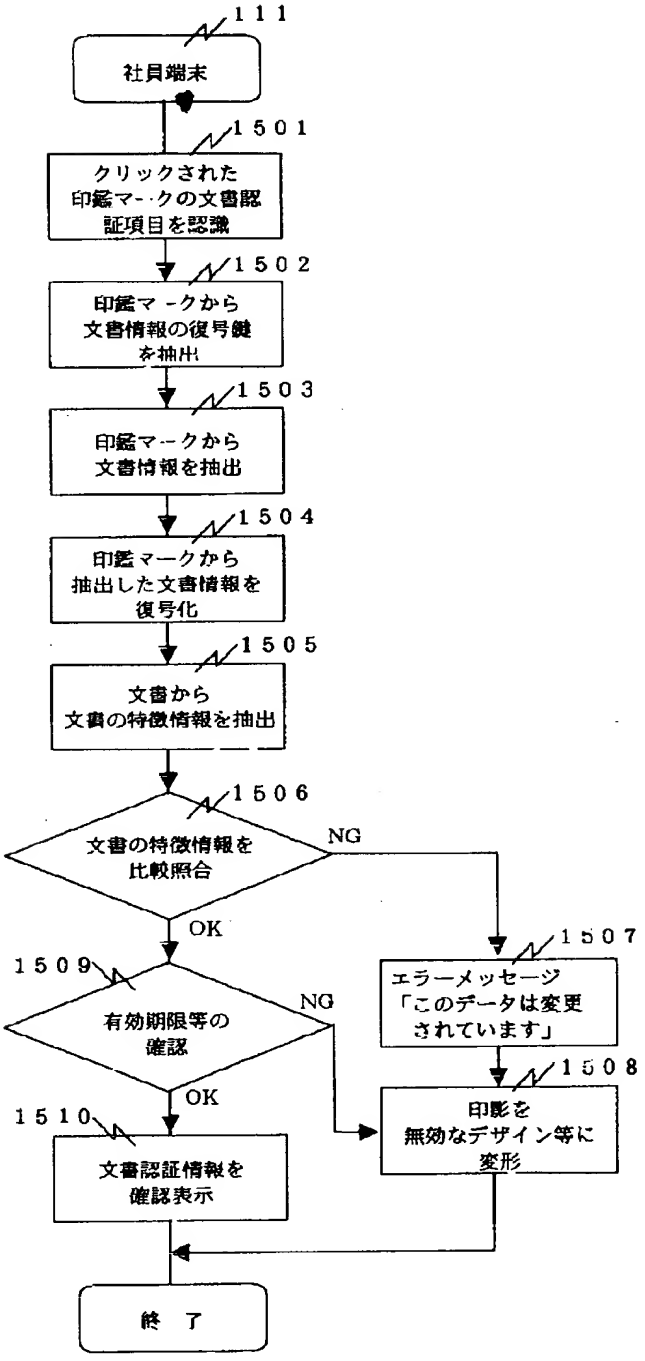
【図14】

図14



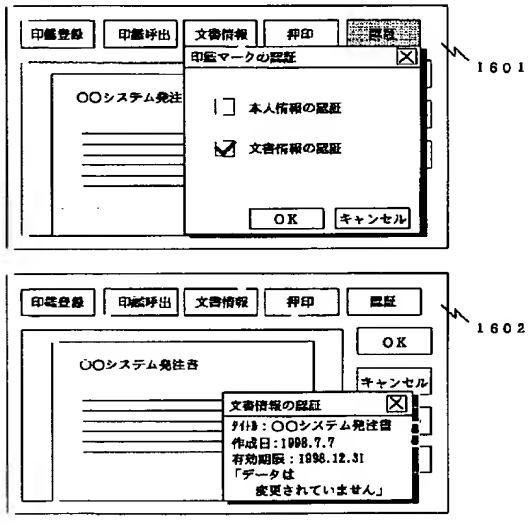

【図15】

図15




【図16】

図16



フロントページの続き

| (51)Int.Cl.[7] | 識別記号 | FI | (参考) |
|---|---|---|---|
| | | H04L 9/00 | 675D |

(72)発明者 永井 康彦
神奈川県川崎市麻生区王禅寺1099番地 株式会社日立製作所システム開発研究所内

Fターム(参考) 5B043 AA09 BA06 BA09 CA10 FA02 FA03 FA07 FA08 GA18
5B049 EE05 EE09 FF03 FF04 GG04 GG07 GG10
5J104 AA07 AA09 AA14 LA06 MA03 PA07